US-CERT Cyber Security Bulletin

SB04-175 *June 23, 2004*

Information previously published in CyberNotes has been incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

Bugs, Holes & Patches

The following tables provide a summary of software vulnerabilities identified between June 6 and June 21, 2004. The tables provides the risk, vendor and software name, potential vulnerability/impact, any identified patches/workarounds/alerts and whether attacks have utilized this vulnerability or an exploit script is known to exist and the common name/CVE number. Software versions and operating systems are identified if known. The tables are organized by operating system with new information identified first followed by updated information. ***Updates to items appearing in previous issues of CyberNotes/Cyber Security Bulletins are listed in bold. New information contained in the update will appear in italicized colored text.*** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures. *Note: All the information included in the following tables has been discussed in newsgroups and websites.*

Windows Operating Systems

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	AspDotNetStore front[1] AspDotNetStore front 3.3, PRO 3.3	Multiple vulnerabilities exist: a Cross-Site Script vulnerability exists in the 'signin.aspx' script due to insufficient sanitization of user-supplied input to the 'returnurl' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'deleteicon.aspx' script due to insufficient restrictions, which could let a remote malicious user delete arbitrary images by providing a valid ProductID; and a vulnerability exists in the 'images.aspx' script due to insufficient validation, which could let a remote malicious user execute arbitrary code. Update available at: http://www.aspdotnetstorefront.com There is no exploit code required; however, Proofs of Concept exploits have been published.	AspDotNet Storefront Multiple Vulnerabilities

[1] Securiteam, June 10, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	ASP-Rider[2] ASP-Rider 1.6	A vulnerability exists when a specially crafted malformed cookie is submitted to a vulnerable site, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	ASP-Rider Administrative Access
High	blosxom.com[3] Blosxom 2.0	A Cross-Site Scripting vulnerability exists in the 'writeback' plugin due to insufficient validation of comments, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Blosxom 'Writeback' Plug-in Cross-Site Scripting
High	IBM[4] eGatherer 2.0 .16	A vulnerability exists in the ActiveX control due to insecure methods ('SetDebugging' and 'RunEgatherer'), which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www-306.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54588 Proofs of Concept exploits have been published.	IBM EGatherer ActiveX Control Dangerous Method
High	IBM[5] acpRunner 1.2.5 .0	A vulnerability exists in the ActiveX control due to insecure methods ('DownLoadURL,' 'SaveFilePath,' and 'Download'), which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www-306.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54588 There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM ACPRunner ActiveX Control Unsafe Methods
High	Microsoft[6] Internet Explorer 5.0, 5.0 for Windows NT 4.0, 98, 95, 2000, 5.0.1, SP1-SP4, 5.0.1 for Windows NT 4.0, 98, 95, 2000, 5.5, SP1&SP2, preview, 6.0, SP1	A Cross-Site Scripting vulnerability exists for sites that have a wildcard DNS entry, which could let a remote malicious user execute arbitrary HTML or script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Internet Explorer Wildcard DNS Cross-Site Scripting

[2] SecurityFocus, June 17, 2004.
[3] Security Advisory KM -2004-01, June 8, 2004.
[4] Securiteam, June 17, 2004.
[5] Securiteam, June 17, 2004.
[6] Bugtraq, June 15, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	PHP Group [7] PHP 4.3.3, 4.3.5	An input validation vulnerability exists in the 'escapeshellcmd()' and 'escapeshellarg()' functions due to insufficient sanitization, which could let a remote malicious user execute arbitrary commands. Upgrades available at: http://www.php.net/downloads.php There is no exploit code required.	PHP escapeshellarg() & escapeshellcmd() Input validation CVE Name: CAN-2004-0542
High	pivotlog.net[8] Pivot Web Log Tool 1.0 02, 1.0, RC1&RC2, Final, 1.0 beta2b, 1.0 beta2, 1.10	Multiple vulnerabilities exist: a vulnerability exists in the 'module_db.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists which could let a remote malicious user write templates with arbitrary extensions to other folders than the intended. Upgrades available at: https://sourceforge.net/project/showfiles.php?group_id=67653&package_id=65955&release_id=245757 There is no exploit code required; however, a Proof of Concept exploit has been published.	Pivot Multiple Vulnerabilities
High	Real Networks[9] RealOne Enterprise Desktop 6.0.11 .774, RealOne Player, 1.0, 2.0, 6.0.11 .872, 6.0.11 .868, 6.0.11 .853, 6.0.11 .841, 6.0.11 .830, 6.0.11 .818, 2.0 for Windows, RealPlayer 10 Japanese, German, English, RealPlayer 8 , RealPlayer Enterprise	Two vulnerabilities exist: a vulnerability exists in 'embd3260.dll' when constructing error messages, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when parsing URLs, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.service.real.com/help/faq/security/040610_player/EN/ Currently we are not aware of any exploits for this vulnerability. Vulnerability has appeared in the press and other public media.	RealPlayer Media File Heap Overflow
High	Real Networks[10] RealPlayer 10, Japanese, German, English	A buffer overflow vulnerability exists due to the way URLs that contain a large number of period characters are handled, which could let a remote malicious user execute arbitrary code. Updates available at: http://service.real.com/help/faq/security/040610_player/EN/ Currently we are not aware of any exploits for this vulnerability. Vulnerability has appeared in the press and other public media.	RealNetworks RealPlayer URI Processing Buffer Overflow

[7] SEC-CONSULT Security Advisory , June 6, 2004.
[8] Securiteam, June 17, 2004.
[9] NGSSoftware Insight Security Research Advisory, NISR11062004, June 11, 2004.
[10] iDEFENSE Security Advisory, June 10, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	Snitz Communications[11] Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3, 3.4 .02-3.4.04	A Cross-Site Scripting vulnerability exists in the 'register.asp' script due to insufficient sanitization of the 'Email' field, which could let a remote malicious user execute arbitrary HTML and script code. Solution available at: http://forum.snitz.com/forum/topic.asp?TOPIC_ID=53360 There is no exploit code required.	Snitz Forums 2000 Cross-Site Scripting
High	Trend Micro[12] OfficeScan Corporate Edition 3.0, 3.5, 3.11, 3.13, 3.54, 5.0 2, 5.5, 5.58	A vulnerability exists in 'winhlp32.exe' because the Windows Help interface is invoked with 'LocalSystem' privileges via the 'OfficeScan Client' window when a virus is detected during real-time scanning, which could let a malicious user execute arbitrary code with SYSTEM privileges. Hotfix information available at: http://uk.trendmicro-europe.com/enterprise/support/knowledge_base_detail.php?solutionId=20118 There is no exploit code required.	OfficeScan 'winhlp32.exe' Arbitrary Code Execution
High	Virtual Programming[13] VP-ASP 4.0, 4.50, 5.0	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'shop$db.asp' and 'shoperror' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exits in the 'shopproductselect.asp' script due to insufficient sanitization of user-supplied input before being used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patch information available at: http://www.vpasp.com/virtprog/info/faq_securityfixes.htm There is no exploit code required; however, Proofs of Concept exploits have been published.	Virtual Programming VP-ASP Multiple Vulnerabilities
High	Web Wiz Guide[14] Web Wiz Forums 7.5, 7.7 b, 7.7 a, 7.8, 7.51	A Cross-Site Scripting vulnerability exists in the 'registration_rules.asp' script due to insufficient sanitization of the 'FID' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.webwizguide.info/web_wiz_forums/forum_download.asp?mode= A Proof of Concept exploit has been published.	Web Wiz Forums 'registration_ rules.asp' Cross-Site Scripting
High/ Medium (Medium if sensitive information can be obtained or corrupted)	Invision Power Services[15] Invision Board 1.3.1 Final	An input validation vulnerability exists in 'ssi.php' due to insufficient validation or user-supplied input, which could let a remote malicious user obtain/modify sensitive information or execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Power Board Input Validation

[11] Secunia Advisory, SA11895, June 21, 2004.
[12] Trend Solution #20118, June 2, 2004.
[13] SecurityTracker Alert, 1010485, June 14, 2004.
[14] SecurityTracker Alert, 1010497, June 16, 2004.
[15] SecurityTracker Alert, 1010448, June 9, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/ Medium (High if arbitrary code can be executed)	NetWin[16] SurgeMail 1.8 g3, 1.8 e, 1.8 d, 1.8 b3, 1.8 a, 1.9 b2, 1.9, 2.0 a2, WebMail 3.1 d	Multiple input validation vulnerabilities exist due to insufficient sanitization of user-supplied data, which could let a remote malicious user obtain sensitive information and execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.netwinsite.com/pub/surgemail/beta/ There is no exploit code required; however, a Proof of Concept exploit has been published.	NetWin SurgeMail/ WebMail Multiple Input Validation
High/ Medium (High if arbitrary code can be executed or admin access obtained; Medium is sensitive information can be obtained)	phpHeaven[17] phpMyChat 0.14.5	Multiple vulnerabilities exist: a vulnerability exists in the 'input.php3' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; multiple SQL injection vulnerabilities exist when SQL syntax is passed through URL parameters of the 'usersL.php3' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'chat/edituser.php3' script, which could let a remote malicious user obtain administrative access; and a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input of the URL parameter passed to the 'admin.php3' script, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHPHeaven PHPMyChat Multiple Remote Vulnerabilities
High/ Medium/ Low (High if arbitrary code can be executed; Medium if sensitive information can be obtained; and Low if a DoS)	Francisco Burzi[18] PHP-Nuke 6.0, 6.5, RC1-RC3, BETA 1, 6.6, 6.7, 6.9, 7.0, FINAL, 7.1-7.3	Multiple vulnerabilities exist: Cross-Site Scripting vulnerabilities exist in the 'Faq,' 'Encyclopedia,' and 'Reviews' modules due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; an input validation vulnerability exists in the 'Reviews' module 'order' parameter due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'preview_review()' function in the 'Reviews' module, which could let a remote malicious user obtain sensitive information; and a Denial of Service vulnerability exists in the 'Review' module score subsystem when a malicious user supplies a large number as a value for a parameter. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHP-Nuke Multiple Input Validation

[16] Secunia Advisory, SA11772, June 7, 2004.
[17] SecurityTracker Alert, 1010515, June 17, 2004.
[18] waraxe-2004-SA#032, June 11, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/Low (Low if a DoS)	Epic Games[19] ARUSH Devastation 390.0; DreamForge TNN; Outdoors Pro Hunter; Epic Games Unreal Engine 436, 433, 226f, Unreal Tournament 451b, 2003 2225 win32, 2225 macOS, 2199 win32, 2199 macOS, 2199 linux, 2004 win32, macOS; nfogrames TacticalOps 3.4 Infogrames X-com Enforcer; Ion Storm DeusEx 1.112 fm; Nerf Arena Blast Nerf Arena Blast 1.2; Rage Software Mobile Forces 20000.0; Robert Jordan Wheel of Time 333.0 b; Running With Scissors Postal 2 1337	A buffer overflow vulnerability exists when a specially crafted secure query is submitted via UDP with a long 'query' value, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Patches available at:: Unreal Tournament 2004 win32 http://www.atari-webcenter.com/friends/?module=friends&action=viewDownloadPage&id=120 Epic Games Unreal Tournament 2004 macOS: http://www.atari-webcenter.com/friends/?module=friends&action=viewDownloadPage&id=120 A Proof of Concept exploit has been published.	Epic Games Unreal Engine 'Secure" Query Buffer Overflow

[19] SecurityTracker Alert, 1010535, June 18, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	BEA Systems, Inc.[20] WebLogic Express 6.1, SP1-SP6, 7.0.0.1, SP1-SP4, 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Express for Win32 6.1, SP1-SP 6, 7.0 .0.1, SP1&SP2, 7.0, SP1-SP5, 8.1, SP1&SP2, Weblogic Server 6.1, SP1-SP6, 7.0.0.1, SP1-SP4, 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Server for Win32 6.1, SP1-SP 6, 7.0 .0.1, SP1&SP2, 7.0, SP1-SP5, 8.1, SP1&SP2	A vulnerability exists due to an error when a client logs into WebLogic Server multiple times as different users using RMI (Remote Method Invocation) over IIOP (Internet Inter-ORB Protocol), which could let a malicious user obtain elevated privileges. The vendor has released updated documentation to address this issue. Customers are advised to read the updated documentation and ensure that client code is written correctly. Updated documentation is available at the following locations: For WebLogic Server and WebLogic Express 8.1: http://e-docs.bea.com/wls/docs81/jndi/jndi.html#478033 For WebLogic Server and WebLogic Express 7.0: http://e-docs.bea.com/wls/docs70/jndi/jndi.html#477188 For WebLogic Server and WebLogic Express 6.1: http://e-docs.bea.com/wls/docs61/jndi/jndi.html#477126 There is no exploit code required.	BEA WebLogic Server & WebLogic Express Java RMI Incorrect Session Inheritance
Medium	Check Point Software[21] Firewall-1 4.0, SP1-SP8, 4.1, SP1-SP6, Next Generation, FP3, HF1&HF2, FP2, FP1, NG-AI R55, NG-AI R54, NG-AI	An information disclosure vulnerability exists during the Internet Key Exchange (IKE) phase due to a design error, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Check Point Firewall-1 Internet Key Exchange Information Disclosure

[20] Security Advisory , BEA04-62.00, June 14, 2004.
[21] Bugtraq, June 16, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	Invision Power Services [22] Invision Board 1.3, Final, 1.3.1 Final	A vulnerability exists when a proxy is used to access a remote forum, which could let a remote malicious user spoof the IP address. No workaround or patch available at time of publishing. There is no exploit code required.	Invision Power Board Potential IP Address Spoofing
Medium	jcifs.samba.org[23] jCIFS 0.6.6, 0.6.8, 0.7 0b5, 0.7-0.7.3, 0.8.1-0.8.3, 0.9 .0b, 0.9 .0	A vulnerability exists if the 'guest' account is enabled on a CIFS server because it is possible to authenticate with any username, which could let a remote malicious user obtain unauthorized access. Upgrades available at: http://jcifs.samba.org/src/jcifs-0.9.2.tgz There is no exploit code required.	jCIFS Authentication Invalid Username
Medium	Microsoft [24] Apple Opera Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, SP1 & SP2, 6.0, SP1; Internet Explorer Macintosh Edition 5.0 MRJ 2.2, MRJ 2.1.4, 5.0, 5.1, 5.1.1, 5.2.2; Opera Software Opera Web Browser 7.51	A vulnerability exists due to an error when handling URLs, which could let a remote malicious user bypass security zones or conduct phishing attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer URI Obfuscation
Medium	Mozilla[25] Mozilla Browser 1.6, 1.7 rc3, Firefox 0.8, 0.9 rc	A vulnerability exits due to an error in the handling of URLs, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Mozilla Browser URI Obfuscation
Medium	Sygate[26] Security Agent 3.0, 3.5 build 2576, Personal Firewall 5.5 build 2576	A vulnerability exists because the kernel-space NDIS driver does not verify the origin of messages that are received through the associated device, which could let a malicious user disable the firewall 'fail-closed' functionality. The vendor has released updates to address this issue. Please contact the vendor to obtain fixes. A Proof of Concept exploit script has been published.	Sygate Personal Firewall Pro Local Fail-Close Bypass

[22] SecurityFocus, June 16, 2004.
[23] SecurityFocus, June 8, 2004.
[24] Bugtraq, June 10, 2004.
[25] SecurityFocus, June 14, 2004.
[26] SIG^2 Vulnerability Research Advisory, June 13, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	The Ignition Project[27] IgnitionServer 0.3.1	A vulnerability exists in the ignitionServer server linking functionality due to missing password verification, which could let a remote malicious user bypass authentication. Upgrade available at: http://www.ignition-project.com/ignition/server/download/ There is no exploit code required.	ignitionServer Server Link Service Authentication Bypass
Medium/ Low (Low if a DoS)	Codemasters Software Company Limited[28] ToCA Race Driver	Multiple remote Denial of Service vulnerabilities exist: a vulnerability exists when a message packet with a length identifier of 0 is submitted; a vulnerability exists when a malformed packet is submitted; and a vulnerability exists because a remote authenticated malicious user can spoof messages that will appear to come from an arbitrary game user. No workaround or patch available at time of publishing. Exploit script has been published.	ToCA Race Driver Multiple Remote Denial of Service
Low	BEA Systems, Inc.[29] WebLogic Express 8.1, SP1&SP2, WebLogic Express for Win32 8.1, SP1&SP2, Weblogic Server 8.1, SP1&SP2, WebLogic Server for Win32 8.1, SP1&SP2	A remote Denial of Service vulnerability due to an error when handling SSL connections. Patches available at: ftp://ftpna.beasys.com/pub/releases/security/CR133071_81sp2.jar Currently we are not aware of any exploits for this vulnerability.	BEA WebLogic Server & WebLogic Express Remote Denial of Service

[27] Securiteam, June 17, 2004.
[28] Securiteam, June 14, 2004.
[29] Security Advisory , BEA04-61.00, June 14, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	IBM[30] Directory Server 4.1, 5.1, HTTP Server 1.3.12-1.3.12 .7, 1.3.19-1.3.19 .5, 1.3.26-1.3.26 .2, 2.0.42, 2.0.42.2, 2.0.47, Tivoli Access Manager for Business Integration 5.1, Manager for e-business 3.9, 4.1, 5.1, WebSphere MQ 5.3 .0.5, 5.3 .0.1, MQ 5.3	A remote Denial of Service vulnerability exists due to an error in the IBM Global Security Toolkit (GSKit) during SSL handshakes. Updates available at: http://www-1.ibm.com/support/docview.wss?uid=swg21169222 Currently we are not aware of any exploits for this vulnerability.	IBM GSKit SSL Handshake Remote Denial of Service
Low	Microsoft[31] Internet Explorer 6.0, SP1	A remote Denial of Service vulnerability exists when a malicious user attempts to invoke the 'Save As' option on a malicious HREF URI. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Internet Explorer HREF 'Save As' Remote Denial of Service

[30] Secunia Advisory, SA11783, June 7, 2004.
[31] Bugtraq, June 15, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	Multiple Vendors[32] AVG Clam AntiVirus Computer Associates Dr. Web Frisk Software McAfee Panda RAV Symantec AVG Anti-Virus 7.0.251; Clam Anti-Virus ClamAV 0.70; Computer Associates eTrust Antivirus 6.0, InoculateIT 6.0; Dr.Web; Frisk Software F-Prot Antivirus for Linux and BSD 4.4.2; McAfee UVscan scan for Linux 4.3.20 McAfee VirusScan 6.0, VirusScan Enterprise 7.1; Panda Antivirus Platinum 2.0; RAV AntiVirus Online Virus Scan; Symantec AntiVirus for Handhelds 3.0, Norton AntiVirus 2002, 2002 Professional Edition, Norton Antivirus 2003, 2003 Professional Edition, Norton AntiVirus Corporate Edition 7.60.build 926	A remote Denial of Service vulnerability exists when certain malicious archives that contain large quantities of data are scanned. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Multiple Vendor Anti-Virus Scanner Remote Denial of Service
Low	Sygate[33] Sygate Personal Firewall Pro 5.5	A Denial of Service vulnerability exists in the 'smc.exe' service using the 'listView' Control. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Sygate Personal Firewall Pro Denial of Service

[32] Bugtraq, June 14, 2004.
[33] SIG^2 Vulnerability Research Advisory, June 13, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	WinAgents Software Group[34] TFTP Server 3.0	A remote Denial of Service vulnerability exists due to a lack of sufficient boundary checks performed on filenames. No workaround or patch available at time of publishing. Exploit script has been published.	WinAgents TFTP Server Remote Buffer Overflow
High	**Microsoft[35]** **Internet Explorer 6.0, SP1** ***US-CERT issues advisories[36, 37]***	**A vulnerability exists because it is possible to pass a dynamically created Iframe to a modal dialog, which could let a remote malicious user execute arbitrary code.** **No workaround or patch available at time of publishing.** **A Proof of Concept exploit has been published. Exploits are also circulating in the wild.**	**Internet Explorer Modal Dialog Zone Bypass** **CVE Name: CAN-2004-0549**
High	**Multiple Vendors[38]** **Active state ActivePerl 5.6.1 .630, 5.6.1- 5.6.3, 5.7.1- 5.7.3, 5.8-5.8.3, 5.9 dev; Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.3** ***US-CERT issues advisory[39]***	**A buffer overflow vulnerability exists in the 'win32_stat()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.** **Activestate:** **http://public.activestate.com/cgi-bin/** **Currently we are not aware of any exploits for this vulnerability.**	**Perl 'win32_stat()' Function Remote Buffer Overflow** **CVE Name: CAN-2004-0377**
High	**Oracle Corporation[40]** **Oracle Applications 11.0, E-Business Suite 11.0, E-Business Suite 11i 11.5.1-11.5.8** ***US-CERT issues advisory[41]***	**Multiple vulnerabilities exist due to input validation errors, which could let a remote malicious user execute arbitrary code.** **Patches available at:** **http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=274375.1** **There is not exploit code required.**	**Oracle E-Business Suite Multiple Input Validation**

[34] SecurityTracker Alert, 1010464, June 10, 2004.
[35] Bugtraq, June 7, 2004.
[36] TA04-163A, http://www.us-cert.gov/cas/techalerts/TA04-163A.html.
[37] VU#713878, http://www.kb.cert.org/vuls/id/713878.
[38] SecurityFocus, April 5, 2004.
[39] VU#722414, http://www.kb.cert.org/vuls/id/722414.
[40] Oracle Security Alert 67, June 3, 2004.
[41] TA04-160A, http://www.us-cert.gov/cas/techalerts/TA04-160A.html.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	Gallery Project[42] Debian[43] *Gentoo*[44] Debian Linux 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gallery Gallery 1.4 -pl1-pl2, 1.4-1.4.3 -pl1 *Gentoo issues advisory*	A vulnerability exists due to an authentication error, which could let a remote malicious user obtain administrative access. Upgrades available at: http://prdownloads.sourceforge.net/gallery/gallery-1.4.3-pl2.tar.gz?download Debian: http://security.debian.org/pool/updates/main/g/gallery/ There is not exploit code required. *Gentoo:* http://security.gentoo.org/glsa/glsa-200406-10.xml	Gallery 'init.php' Authentication Flaw

[42] Gallery Security Release, June 1, 2004.
[43] Debian Security Advisory, DSA 512-1, June 2, 2004.
[44] Gentoo Linux Security Advisory , GLSA 200406-10, June 15, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/ Medium/ Low/ (Low if a DoS; Medium if elevated privileges obtained; and High if arbitrary code can be executed)	**Microsoft**[45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59] **Windows NT Work-station 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Net-Meeting, Windows 98, SE, ME;** ***Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messaging, S8100 Media Servers*** ***Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnerability***[60] ***More exploits published***[61] ***Microsoft re-releases bulletin***[62]	**A vulnerability exists in LSASS, which could let a remote malicious user execute arbitrary code; a DoS vulnerability exists in LSASS when processing LDAP requests; a vulnerability exists in the PCT protocol, which could let a remote malicious user execute arbitrary code; a vulnerability exists in Winlogon, which could let a remote malicious user execute arbitrary code; a vulnerability exists when rendering Metafiles, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'Help and Support Center' when handling HCP URLs, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the Utility Manager, which could let a remote malicious user obtain SYSTEM privileges; a vulnerability exists in Windows task management, which could let a remote malicious user execute arbitrary code; a vulnerability exists when creating entries in the Local Descriptor Table, which could let a malicious user obtain elevated privileges; a vulnerability exists in the H.323 protocol, which could let a malicious user execute arbitrary code; a vulnerability exists in the Virtual DOS Machine subsystem, which could let a malicious user obtain elevated privileges; a DoS vulnerability exists in Negotiate Security Software Provider, which could also let a remote malicious user execute arbitrary code; a DoS vulnerability exists in the SSL library & ASN.1 Library, which could also let a malicious user execute arbitrary code.** **Frequently asked questions regarding this vulnerability and the patch can be found at:** **http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx** ***Exploit script has been published for the PCT protocol vulnerably.*** ***Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.*** ***More exploit scripts have been published. A White paper has been also published that analyzes the SSL PCT vulnerability and gives full details on how exploitation has been performed and what it takes for working exploits to be created.*** ***Bulletin updated to advise on the availability of an updated Windows NT 4.0 Workstation update for the Pan Chinese language. This update should be installed by customers even if the original update was installed.***	**Microsoft Windows Multiple Vulnerabilities** **CVE Names: CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906, CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2003-0117, CAN-2003-0118, CAN-2003-0119, CAN-2004-0120, CAN-2004-0123**

[45] Microsoft Security Bulletin, MS04-011, April 13, 2004.
[46] VU#260588, http://www.kb.cert.org/vuls/id/260588.
[47] VU#150236, http://www.kb.cert.org/vuls/id/150236.
[48] VU#255924, http://www.kb.cert.org/vuls/id/255924.
[49] VU#638548, http://www.kb.cert.org/vuls/id/638548.
[50] VU#783748, http://www.kb.cert.org/vuls/id/783748.
[51] VU#353956, http://www.kb.cert.org/vuls/id/353956.
[52] VU#122076, http://www.kb.cert.org/vuls/id/122076.
[53] VU#206468, http://www.kb.cert.org/vuls/id/206468.
[54] VU#526084, http://www.kb.cert.org/vuls/id/526084.
[55] VU#547028, http://www.kb.cert.org/vuls/id/547028.
[56] VU#639428, http://www.kb.cert.org/vuls/id/639428.
[57] VU#471260, http://www.kb.cert.org/vuls/id/471260.
[58] VU#753212, http://www.kb.cert.org/vuls/id/753212.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/Low **(High if arbitrary code can be executed)**	**Firebird**[63] ***Borland/Inprise*** **Firebird 1.0** ***Borland/Inprise Interbase 4.0, 5.0, 6.0, 6.4, 6.5, 7.0, 7.1, InterBase SuperServer 6.0*** ***Exploit script published***[64]	**A buffer overflow vulnerability exists when handling database names due to insufficient boundary checks, which could let a remote malicious user cause a Denial of Service and ultimately execute arbitrary code.** **Upgrade available at: http://firebird.sourceforge.net/index.php?op=files&id=engine** **A Proof of Concept exploit has been published.**	**Firebird Remote Database Name Buffer Overflow**
Medium	**BEA Systems Inc.**[65] **WebLogic Server and WebLogic Express** ***US-CERT issues advisory***[66]	**A vulnerability that occurs when a weblogic.xml file is edited through Weblogic Builder or the SecurityRoleAssignmentMBean may allow unintended access to web applications.** **Patch available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_59.00.jsp**	**Weblogic & Web Express Unauthorized Access** **CVE Name: CAN-2004-0470**

Unix Operating Systems

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	blosxom.com[67] Blosxom 2.0	A Cross-Site Scripting vulnerability exists in the 'writeback' plugin due to insufficient validation of comments, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Blosxom 'Writeback' Plug-in Cross-Site Scripting
High	cPanel, Inc.[68] cluecentral suexec.patch	Several vulnerabilities exist: a vulnerability exists in the cPanel patch to the Apache suEXEC when configured for 'mod_php,' which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	cPanel 'mod_php' suEXEC Trait

[59] VU#586540, http://www.kb.cert.org/vuls/id/586540.
[60] SecurityFocus, April 21, 2004.
[61] Packetstorm, May 4, 2004
[62] Microsoft Security Bulletin, MS04-011 V2.0 June 15, 2004.
[63] Securiteam, June 1, 2004.
[64] SecurityFocus, June 12, 2004.
[65] BEA Security Advisory: (BEA04-59.00), May 11, 2004
[66] VU#950070, http://www.kb.cert.org/vuls/id/950070.
[67] Security Advisory KM -2004-01, June 8, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	cPanel, Inc.[69] cPanel 5.0, 5.3, 6.0, 6.2, 6.4- 6.4.2, 7.0, 8.0, 9.0, 9.1 .0-R85, 9.1	A vulnerability exits in multiple Perl scripts that are distributed with cPanel because scripts do not run with taint mode, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	CPanel Perl Script Failure To Implement Taint Mode
High	Debian[70] Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; sup sup 1.8	A format string vulnerability exists because 'syslog(3)' calls in the 'logquit,' 'logerr,' and 'loginfo' functions are made without the appropriate format string specifiers, which could let a remote malicious user execute arbitrary code. **Debian:** http://security.debian.org/pool/updates/main/s/sup/ Currently we are not aware of any exploits for this vulnerability.	Sup Remote Syslog Format String CVE Name: CAN-2004-0451
High	Epic Games[71] ARUSH Devastation 390.0; DreamForge TNN; Outdoors Pro Hunter; Epic Games Unreal Engine 436, 433, 226f, Unreal Tournament 451b, 2003 2225 win32, 2225 macOS, 2199 win32, 2199 macOS, 2199 linux, 2004 win32, macOS; nfogrames TacticalOps 3.4 Infogrames X-com Enforcer; Ion Storm DeusEx 1.112 fm; Nerf Arena Blast Nerf Arena Blast 1.2; Rage Software Mobile Forces 20000.0; Robert Jordan Wheel of Time 333.0 b; Running With Scissors Postal 2 1337	A buffer overflow vulnerability exists when a specially crafted 'Secure' query is submitted via UDP with a long 'query' value, which could let a remote malicious user cause a Denial of Service and execute arbitrary code. Patches available at:: Unreal Tournament 2004 win32 http://www.atari-webcenter.com/friends/?module=friends&action=viewDownloadPage&id=120 Epic Games Unreal Tournament 2004 macOS: http://www.atari-webcenter.com/friends/?module=friends&action=viewDownloadPage&id=120 A Proof of Concept exploit has been published.	Epic Games Unreal Engine 'Secure" Query Buffer Overflow

[68] SecurityTracker Alert, 1010411, June 7, 2004.
[69] SecurityTracker Alert, 1010411, June 7, 2004.
[70] Debian Security Advisory, DSA 521-1, June 19, 2004.
[71] SecurityTracker Alert, 1010535, June 18, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	GNU[72] Gentoo[73] Aspell 0.50.5; Gentoo Linux 1.4	A buffer overflow vulnerability exists in the 'word-list-compress' utility due to insufficient bounds checking, which could let a malicious user execute arbitrary code. **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-14.xml Proofs of Concept exploits have been published.	GNU Aspell Stack Buffer Overflow CVE Name: CAN-2004-0547
High	Hewlett Packard Company[74] HP-UX 11.x	A buffer overflow vulnerability exists in Xfs due to insufficient validation of the length of a user-supplied string before copying it into a finite buffer, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. Exploit script has been published.	HP-UX Local X Font Server Buffer Overflow
High	Horde Project[75] Caldera Conectiva Debian Gentoo[76] IMP 2.0, 2.2-2.2.8, 2.3, 3.0 Horde IMP 3.1 Horde IMP 3.1.2 Horde IMP 3.2-3.2.3	A Cross-Site Script vulnerability exists in the 'Content-type' header due to insufficient filtering of data in e-mail messages, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://ftp.horde.org/pub/imp/imp-3.2.4.tar.gz **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-11.xml There is no exploit code required.	Horde IMP Cross-Site Scripting
High	Horde Project[77] Gentoo[78] Horde Chora 1.2.1; Gentoo Linux 1.4	A vulnerability exists due to insufficient validation of a user-supplied variable (the number of diff context lines) before constructing an 'exec()' call based on the variable, which could let a remote malicious user execute arbitrary code. Upgrade available at: ftp://ftp.horde.org/pub/chora/chora-1.2.2.tar.gz **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-09.xml Currently we are not aware of any exploits for this vulnerability.	Chora Input Validation

[72] Securiteam, June 14,2 004.
[73] Gentoo Linux Security Advisory, GLSA 200406-14, June 17, 2004.
[74] SecurityTracker Alert, 1010529, June 18, 2004.
[75] SecurityFocus, June 9, 2004.
[76] Gentoo Linux Security Advisory , GLSA 200406-11, June 16, 2004.
[77] e-matters GmbH Security Advisory, June 13, 2004.
[78] Gentoo Linux Security Advisory , GLSA 200406-09, June 15, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	Jamie Cameron[79] Gentoo[80] Usermin 1.0 70	A Cross-Site Scripting vulnerability exists in the web mail module due to insufficient sanitization of HTML email messages, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://www.webmin.com/udownload.html **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-15.xml There is no exploit code required.	Usermin Cross-Ste Scripting
High	MoinMoin[81] MoinMoin 1.1, 1.2, 1.2.1	A vulnerability exists because remote web clients can create their own user accounts without administrative intervention or approval, which could let a remote malicious user obtain administrative privileges. Upgrades available at: http://prdownloads.sourceforge.net/moin/moin-1.2.2.tar.gz?download There is no exploit code required.	MoinMoin Group Name Privilege Escalation
High	Multiple Vendors[82] Astaro Caldera Conectiva CRUX Debian Gentoo Mandrake RedHat Slackware Sun SuSE TurboLinux WOLK Linux kernel 2.4-2.4.20, 2.5.0-2.5.69	An integer overflow vulnerability exists in the inter integrated circuit (I2C) bus driver due to insufficient validation of user-reported size values, which could let a malicious user execute arbitrary code with kernel-level privileges. Upgrades available at: http://www.kernel.org/pub/linux/kernel/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Integer Overflow in i2c Driver

[79] SNS Advisory No.73, June 11, 2004.
[80] Gentoo Linux Security Advisory , GLSA 200406-15, June 18, 2004.
[81] Securiteam, June 17, 2004.
[82] SecurityTracker Alert, 1010512, June 17, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	pivotlog.net[83] Pivot Web Log Tool 1.0 02, 1.0, RC1&RC2, Final, 1.0 beta2b, 1.0 beta2, 1.10	Multiple vulnerabilities exist: a vulnerability exists in the 'module_db.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists which could let a remote malicious user write templates with arbitrary extensions to other folders than the intended. Upgrades available at: https://sourceforge.net/project/showfiles.php?group_id=67653&package_id=65955&release_id=245757 There is no exploit code required; however, a Proof of Concept exploit has been published.	Pivot Multiple Vulnerabilities
High	rlpr Debian[84] rlpr 2.0 1-2.0.4, 2.0	Multiple vulnerabilities exist: a format string vulnerability exists in the 'msg()' function due to a syslog(3) call made without the proper format string specifier, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'msg()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. **Debian:** http://security.debian.org/pool/updates/main/r/rlpr/ Currently we are not aware of any exploits for this vulnerability.	Rlpr Multiple Vulnerabilities CVE Names: CAN-2004-0393, CAN-2004-0454
High	SGI[85] IRIX 6.5.x	A vulnerability exists in the 'syssgi()' system call function 'SGI_IOPROBE' which could let a malicious user obtain Root privileges. Patches available at: ftp://patches.sgi.com/support/free/security/advisories/ Currently we are not aware of any exploits for this vulnerability.	SGI IRIX 'syssgi()' System Call Root Access CVE Name: CAN-2004-0135
High	Snitz Communications[86] Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3, 3.4 .02-3.4.04	A Cross-Site Scripting vulnerability exists in the 'register.asp' script due to insufficient sanitization of the 'Email' field, which could let a remote malicious user execute arbitrary HTML and script code. Solution available at: http://forum.snitz.com/forum/topic.asp?TOPIC_ID=53360 There is no exploit code required.	Snitz Forums 2000 Cross-Site Scripting

[83] Securiteam, June 17, 2004.
[84] Debian Security Advisory, DSA 524-1, June 19, 2004.
[85] SGI Security Advisory , 20040601-01-P, June 14, 2004.
[86] Secunia Advisory, SA11895, June 21, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	Squid-cache.org Debian Fedora[87] Gentoo[88] Mandrake[89] OpenPKG RedHat[90] SGI[91] SuSE[92] Tinysofa[93] Trustix[94] Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.4 STABLE7, 2.4. 2.5 STABLE5, STABLE4, STABLE3, STABLE1	A buffer overflow vulnerability exists in 'helpers/ntlm_auth/SMB/libntlmssp.c' in the 'ntlm_check_auth()' function due to insufficient validation, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.squid-cache.org/~wessels/patch/libntlmssp.c.patch **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-13.xml **Mandrake:** http://www.mandrakesoft.com/security/advisories **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-242.html **SGI:** ftp://patches.sgi.com/support/free/security/advisories/ **SuSE:** ftp://ftp.suse.com/pub/suse/i **Tinysofa:** http://http.tinysofa.org/pub/tinysofa/updates/server-1.0/rpms/squid-2.5.STABLE5-6ts.i586.rpm **Trustix:** http://http.trustix.org/pub/trustix/updates/ Exploit script has been published.	Squid Proxy NTLM Buffer Overflow CVE Name: CAN-2004-0541
High	Wolfgang Zekoll[95] smtp.proxy 1.1.3	A format string vulnerability exists in 'smtp.c' when handling client hostnames and the 'Message-ID:' header, which could let a remote malicious user execute arbitrary code. No workaround or pat ch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	SMTP.Proxy Remote Format String

[87] Fedora Update Notifications, FEDORA-2004-163 & 164, June 9, 2004.
[88] Gentoo Linux Security Advisory, GLSA 200406-13, June 17, 2004.
[89] Mandrakelinux Security Update Advisory, MDKSA-2004:059, June 9, 2004.
[90] RedHat Security Advisory, RHSA-2004:242-06, June 9, 2004.
[91] SGI Security Advisory, 20040604-01-U, June 21, 2004.
[92] SUSE Security Announcement, SuSE-SA:2004:016, June 9, 2004.
[93] Tinysofa Security Advisory, TSSA-2004-010, June 9, 2004.
[94] Trustix Secure Linux Security Advisory, TSLSA-2004-0033, June 10, 2004.
[95] 0xbadc0ded Advisory #04, June 5, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/ Medium (Medium if elevated privileges can be obtained)	Apple[96] Mac OS X 10.2.8, 10.3.4, OS X Server 10.2.8, 10.3.4	Multiple vulnerabilities exist: a vulnerability exists in the 'LaunchServices' utility when automatically registering applications, which could let a remote malicious user register and run malicious applications; a vulnerability exists in 'DiskImageMounter' because the 'disk://URI' handler can be used to mount an anonymous remote file system, which could let a remote malicious user write to the local disk; and a vulnerability exists in Safari in the 'Show in Finder' button, which could let a remote malicious user obtain elevated privileges or execute arbitrary code. Upgrades available at: http://www.apple.com/support/downloads/securityupdate_2004-06-07_(_10_2_8).html http://www.apple.com/support/downloads/securityupdate_2004-06-07_(_10_3_4).html Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X Multiple Security Vulnerabilities CVE Names: CAN-2004-0538, CAN-2004-0539
High/ Medium (Medium if sensitive information can be obtained or corrupted)	Invision Power Services [97] Invision Board 1.3.1 Final	An input validation vulnerability exists in 'ssi.php' due to insufficient validation or user-supplied input, which could let a remote malicious user obtain/modify sensitive information or execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Power Board Input Validation
High/ Medium (High if arbitrary code can be executed)	NetWin[98] SurgeMail 1.8 g3, 1.8 e, 1.8 d, 1.8 b3, 1.8 a, 1.9 b2, 1.9, 2.0 a2, WebMail 3.1 d	Multiple input validation vulnerabilities exist due to insufficient sanitization of user-supplied data, which could let a remote malicious user obtain sensitive information and execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.netwinsite.com/pub/surgemail/beta/ There is no exploit code required; however, a Proof of Concept exploit has been published.	NetWin SurgeMail/ WebMail Multiple Input Validation

[96] Apple Security Update, APPLE-SA-2004-06-07, June 7, 2004.
[97] SecurityTracker Alert, 1010448, June 9, 2004.
[98] Secunia Advisory, SA11772, June 7, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/ Medium (High if arbitrary code can be executed or admin access obtained; Medium is sensitive information can be obtained)	phpHeaven[99] phpMyChat 0.14.5	Multiple vulnerabilities exist: a vulnerability exists in the 'input.php3' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; multiple SQL injection vulnerabilities exist when SQL syntax is passed through URL parameters of the 'usersL.php3' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'chat/edituser.php3' script, which could let a remote malicious user obtain administrative access; and a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input of the URL parameter passed to the 'admin.php3' script, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHPHeaven PHPMyChat Multiple Remote Vulnerabilities
High/ Medium/ Low (High if arbitrary code can be executed; Medium if sensitive information can be obtained; and Low if a DoS)	Francisco Burzi[100] PHP-Nuke 6.0, 6.5, RC1-RC3, BETA 1, 6.6, 6.7, 6.9, 7.0, FINAL, 7.1-7.3	Multiple vulnerabilities exist: Cross-Site Scripting vulnerabilities exist in the 'Faq,' 'Encyclopedia,' and 'Reviews' modules due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; an input validation vulnerability exists in the 'Reviews' module 'order' parameter due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'preview_review()' function in the 'Reviews' module, which could let a remote malicious user obtain sensitive information; and a Denial of Service vulnerability exists in the 'Review' module score subsystem when a malicious user supplies a large number as a value for a parameter. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHP-Nuke Multiple Input Validation
High/Low (Low if a DoS)	Apache Software Foundation[101] Conectiva HP Immunix Mandrake OpenBSD OpenPKG[102] RedHat SGI Trustix Apache 1.3.26-1.3.29, 1.3.31; OpenBSD –current, 3.4, 3.5	A buffer overflow vulnerability exists in Apache mod_proxy when a 'Content Length:' header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://marc.theaimsgroup.com/?l=apache-httpd-dev&m=108687304202140&q=p3 **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **OpenPKG:** ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm A Proof of Concept exploit script has been published.	Apache Mod_Proxy Remote Buffer Overflow CVE Name: CAN-2004-0492

[99] SecurityTracker Alert, 1010515, June 17, 2004.
[100] waraxe-2004-SA#032, June 11, 2004.
[101] SecurityTracker Alert, 1010462, June 10, 2004.
[102] OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/Low (Low if a DoS)	CVS Caldera Conectiva Debian[103] Fedora[104] Gentoo[105] Immunix Mandrake[106] OpenBSD OpenPKG[107] RedHat[108] SGI[109] Slackware SuSE[110] CVS 1.10.7, 1.10.8, 1.11-1.11.6, 1.11.10, 1.11.11, 1.11.14-1.11.16, 1.12.1, 1.12.2, 1.12.5, 1.12.7, 1.12.8; Gentoo Linux 1.4; OpenBSD –current, 3.4, 3.5; OpenPKG Current, 1.3, 2.0	Multiple vulnerabilities exist: a null-termination vulnerability exists regarding 'Entry' lines that was introduced by a previous CVS security patch, which could let a remote malicious user execute arbitrary code; a 'double free' vulnerability exists in the 'Arguments 'command, which could let a remote malicious user execute arbitrary code; a format string vulnerability exists in the processing of the CVS wrapper file, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the handling of the 'Max-dotdot' CVS protocol command, which could let a remote malicious user cause a Denial of Service; a vulnerability exists in the 'serve_notify()' function when handling empty data lines, which could let a remote malicious user execute arbitrary code; several errors exist when reading configuration files containing empty lines from CVSROOT, which could let a remote malicious user cause a Denial of Service; and various integer multiplication overflow vulnerabilities exist, which could let a remote malicious user execute arbitrary code. **CVS:** https://ccvs.cvshome.org/files/documents/19/194/cvs-1.11.17.tar.gz **Debian:** http://security.debian.org/pool/updates/main/c/cvs/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1 **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-06.xml **Mandrake:** http://www.mandrakesoft.com/security/advisories **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **OpenPKG:** ftp://ftp.openpkg.org/release **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-233.html **SGI:** ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ **SuSE:** ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits that are circulating for these vulnerabilities.	CVS Multiple Vulnerabilities CVE Names: CAN-2004-0414, CAN-2004-0416, CAN-2004-0417, CAN-2004-0418

[103] Debian Security Advisories, DSA 517-1 & 519-1, , June 10 & 15, 2004.
[104] Fedora Update Notifications, FEDORA-2004-169 & 170, June 11, 2004.
[105] Gentoo Linux Security Advisory , GLSA 200406-06, June 10, 2004.
[106] Mandrakelinux Security Update Advisory , MDKSA-2004:058, June 9, 2004.
[107] OpenPKG Security Advisory , OpenPKG-SA-2004.027, June 11, 2004.
[108] RedHat Security Advisory, RHSA-2004:233-07, June 9, 2004.
[109] SGI Security Advisories, 20040604-01-U & 20040605-01-U, June 21, 2004.
[110] SUSE Security Announcement, SuSE-SA:2004:015, June 9, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High/Low (High if arbitrary code can be executed)	Insight Distribution Systems Conectiva Debian[111] Gentoo PostgreSQL 7.2.1	A buffer overflow vulnerability exists in 'misc.c' in the 'make_string()' function, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. **Debian:** http://security.debian.org/pool/updates/main/p/postgresql/ Currently we are not aware of any exploits for this vulnerability.	Mkdir Buffer Overflow
High/Low (Low if a DoS)	Subversion Fedora[112] Gentoo[113] OpenPKG[114] SuSE[115] OpenPKG Current, 2.0; Subversion 1.0-1.0.4	A vulnerability exists in the 'svn' protocol parser due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrades available at: http://subversion.tigris.org/tarballs/subversion-1.0.5.tar.gz **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-07.xml **OpenPKG:** ftp://ftp.openpkg.org/release/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ Currently we are not aware of any exploits for this vulnerability.	Subversion SVN Protocol Parser CVE Name: CAN-2004-0413

[111] Debian Security Advisory, DSA 516-1, June 7, 2004.
[112] Fedora Update Notifications, FEDORA-2004-165 & 166, June 14, 2004.
[113] Gentoo Linux Security Advisory, GLSA 200406-07, June 11. 2004.
[114] OpenPKG Security Advisory, OpenPKG-SA-2004.028, June 11. 2004.
[115] SUSE Security Announcement, SuSE-SA:2004:018, June 17, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	BEA Systems, Inc.[116] WebLogic Express 6.1, SP1-SP6, 7.0.0.1, SP1-SP4, 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Express for Win32 6.1, SP1-SP 6, 7.0 .0.1, SP1&SP2, 7.0, SP1-SP5, 8.1, SP1&SP2, Weblogic Server 6.1, SP1-SP6, 7.0.0.1, SP1-SP4, 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Server for Win32 6.1, SP1-SP 6, 7.0 .0.1, SP1&SP2, 7.0, SP1-SP5, 8.1, SP1&SP2	A vulnerability exists due to an error when a client logs into WebLogic Server multiple times as different users using RMI (Remote Method Invocation) over IIOP (Internet Inter-ORB Protocol), which could let a malicious user obtain elevated privileges. The vendor has released updated documentation to address this issue. Customers are advised to read the updated documentation and ensure that client code is written correctly. Updated documentation is available at the following locations: For WebLogic Server and WebLogic Express 8.1: http://e-docs.bea.com/wls/docs81/jndi/jndi.html#478033 For WebLogic Server and WebLogic Express 7.0: http://e-docs.bea.com/wls/docs70/jndi/jndi.html#477188 For WebLogic Server and WebLogic Express 6.1: http://e-docs.bea.com/wls/docs61/jndi/jndi.html#477126 There is no exploit code required.	BEA WebLogic Server & WebLogic Express Java RMI Incorrect Session Inheritance
Medium	Check Point Software[117] Firewall-1 4.0, SP1-SP8, 4.1, SP1-SP6, Next Generation, FP3, HF1&HF2, FP2, FP1, NG-AI R55, NG-AI R54, NG-AI	An information disclosure vulnerability exists during the Internet Key Exchange (IKE) phase due to a design error, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Check Point Firewall-1 Internet Key Exchange Information Disclosure
Medium	cPanel Inc.[118] cPanel 5.0, 5.3, 6.0, 6.2, 6.4-6.4.2, 7.0, 8.0, 9.0, 9.1 .0-R85, 9.1	A vulnerability exists in the 'passwd' script due to insufficient sanitization of user-supplied URI parameter input before using it in an SQL query, which could let a remote malicious user modify passwords for databases. Update available at: http://www.cpanel.net/downloads.htm A Proof of Concept exploit has been published.	cPanel Unauthorized Database Password Changes
Medium	FreeBSD[119] FreeBSD 4.x	A vulnerability exists in 'jail(2)' due to a failure to verify that attempts to modify the routing tables originate from non-jailed processes, which could let a malicious user corrupt the routing table of the server. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:12/jailroute.patch Currently we are not aware of any exploits for this vulnerability.	FreeBSD 'jail(2)' Routing Table Modification CVE Name: CAN-2004-0125

[116] Security Advisory, BEA04-62.00, June 14, 2004.
[117] Bugtraq, June 16, 2004.
[118] SecurityTracker Alert, 1010449, June 9, 2004.
[119] FreeBSD Security Advisory, FreeBSD-SA-04:12, June 7, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	Invision Power Services [120] Invision Board 1.3, Final, 1.3.1 Final	A vulnerability exists when a proxy is used to access a remote forum, which could let a remote malicious user spoof the IP address. No workaround or patch available at time of publishing. There is no exploit code required.	Invision Power Board Potential IP Address Spoofing
Medium	Jamie Cameron [121] Webmin 1.140	An information disclosure vulnerability exists due to an access validation error, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://prdownloads.sourceforge.net/webadmin/webmin-1.150.tar.gz Currently we are not aware of any exploits for this vulnerability.	Webmin Configuration Module Information Disclosure
Medium	Jamie Cameron [122] Gentoo[123] Usermin 1.0 70; Webmin 1.140	A vulnerability exists in the account lockout mechanism due to insufficient validation of user-supplied input and improper parsing of certain characters, which could let a remote malicious user attempt to guess IDs and passwords continuously and prevent legitimate users from logging on. Upgrades available at: **Usermin:** http://www.webmin.com/udownload.html **Webmin:** http://prdownloads.sourceforge.net/webadmin/webmin-1.150.tar.gz There is no exploit code required.	Webmin & Usermin Account Lockout Bypass
Medium	jcifs.samba.org[124] jCIFS 0.6.6, 0.6.8, 0.7 0b5, 0.7-0.7.3, 0.8.1-0.8.3, 0.9 .0b, 0.9 .0	A vulnerability exists if the 'guest' account is enabled on a CIFS server because it is possible to authenticate with any username, which could let a remote malicious user obtain unauthorized access. Upgrades available at: http://jcifs.samba.org/src/jcifs-0.9.2.tgz There is no exploit code required.	jCIFS Authentication Invalid Username
Medium	KAME Project[125] IPsec-Tools 0.3, rc1-rc5, 0.3.1, 0.3.2; KAME Racoon, 20040503, 20040407b, 20040405, 20030711	A vulnerability exists due to an authentication error in the 'eay_check_x509cert()' function when verifying certificates, which could lead to the validation of invalid certificates. Upgrades available at: http://prdownloads.sourceforge.net/ipsec-tools/ipsec-tools-0.3.3.tar.gz?download There is no exploit code required.	KAME Racoon X.509 Certificate Validation

[120] SecurityFocus, June 16, 2004.
[121] SNS Advisory No.74, June 11, 2004.
[122] SNS Advisory No.75, June 11, 2004.
[123] Gentoo Linux Security Advisory, GLSA 200406-12, June 16, 2004.
[124] SecurityFocus, June 8, 2004.
[125] Bugtraq, June 14, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	Microsoft[126] Apple Opera Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, SP1 & SP2, 6.0, SP1; Internet Explorer Macintosh Edition 5.0 MRJ 2.2, MRJ 2.1.4, 5.0, 5.1, 5.1.1, 5.2.2; Opera Software Opera Web Browser 7.51	A vulnerability exists due to an error when handling URLs, which could let a remote malicious user bypass security zones or conduct phishing attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer URI Obfuscation
Medium	Multiple Vendors Astaro Conectiva Debian Devil-Linux Mandrake RedHat[127] Slackware SuSE TurboLinux Trustix[128] Linux kernel 2.4.18, 2.4.19, 2.4.21-2.4.26, 2.6-2.6.7	Vulnerabilities exist in various drivers (aironet, asus_acpi, decnet, mpu401, msnd, and pss) for the Linux kernel, which could let a malicious user obtain sensitive information or elevated privileges. Update available at: http://www.kernel.org/ **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-255.html **Truxtix:** ftp://ftp.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Multiple Device Drivers CVE Name: CAN-2004-0495
Medium	Roundup[129] Roundup 0.5-0.5.9, 0.6.11	A Directory Traversal vulnerability exists due to an input validation error in the web interface when processing HTTP requests, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/roundup/roundup-0.7.3.tar.gz?download There is no exploit code required; however, a Proof of Concept exploit has been published.	Roundup Directory Traversal

[126] Bugtraq, June 10, 2004.
[127] RedHat Security Advisory, RHSA-2004:255-10, June 17, 2004.
[128] Trustix Secure Linux Security Advisory, TSLSA-2004-0035, June 18, 2004.
[129] SourceForge Tracker Detail 961511, June 8, 200.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	Symantec[130] Enterprise Firewall 8.0	A vulnerability exists win the integrated DNS proxy when acting as a caching DNS server, which could let a remote malicious user deny service to legitimate users by redirecting traffic to inappropriate hosts, perform man-in-the-middle attacks, and impersonate sites. Updates available at: http://securityresponse.symantec.com/avcenter/security/Content/2004.06.21.html Proof of Concept exploit scripts have been published.	Symantec Enterprise Firewall DNSD DNS Cache Poisoning
Medium/ Low (Low if a DoS)	GNU Mandrake[131] Ksymoops 2.4.5, 2.4.8, 2.4.9; MandrakeSoft Corporate Server 2.1 x86_64, 2.1, Linux Mandrake 9.1, ppc, 9.2, amd64, 10.0, AMD64	A vulnerability exists because the 'ksymoops-gznm' script copies files to the "/tmp" directory insecurely, which could let a malicious user cause a Denial of Service or modify user/system information. **Mandrake:** http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	'ksymoops-gznm' Insecure Temporary File Handling
Medium/ Low (Medium is sensitive information can be obtained)	Jamie Cameron[132] Caldera Gentoo[133] HP Mandrake RedHat SCO Webmin 0.1-0.7, 0.8.3-0.8.5, 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.89, 0.91-0.99, 1.0 90, 1.0 80, 1.0 70, 1.0 60, 1.0 50, 1.0 20, 1.0 00, 1.110, 1.121, 1.130, 1.140	Two vulnerabilities exist: a vulnerability exists which could let an unauthenticated remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user submits an incorrect username or passwords. Upgrades available at: http://prdownloads.sourceforge.net/webadmin/webmin-1.150.tar.gz **Gentoo:** http://security.gentoo.org/glsa/glsa-200406-12.xml There is no exploit code required.	Webmin Multiple Remote Vulnerabilities

[130] Symantec Security Advisory, SYM04-010, June 21, 2004.
[131] Mandrakelinux Security Update Advisory, MDKSA-2004:060, June 10, 2004.
[132] Secunia Advisory, SA11794, June 7, 2004.
[133] Gentoo Linux Security Advisory, GLSA 200406-12, June 16, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	BEA Systems, Inc.[134] WebLogic Express 8.1, SP1&SP2, WebLogic Express for Win32 8.1, SP1&SP2, Weblogic Server 8.1, SP1&SP2, WebLogic Server for Win32 8.1, SP1&SP2	A remote Denial of Service vulnerability due to an error when handling SSL connections. Patches available at: ftp://ftpna.beasys.com/pub/releases/security/CR133071_81sp2.jar Currently we are not aware of any exploits for this vulnerability.	BEA WebLogic Server & WebLogic Express Remote Denial of Service
Low	FreeIPS[135] FreeIPS 1.0	A remote Denial of Service vulnerability exists when a user submits a malicious string pattern. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	FreeIPS Protected Service Remote Denial of Service
Low	Gergely Nagy[136] Thy HTTP Daemon 0.9 .0-0.9.2	A remote Denial of Service vulnerability exists in 'src/session.c' in the '_session_parse_absoluteuri()' function. Update available at: http://bonehunter.rulez.org/Thy.phtml There is no exploit code required.	Thy HTTP Daemon Remote Denial of Service

[134] Security Advisory , BEA04-61.00, June 14, 2004.
[135] SecurityFocus, June 17, 2004.
[136] SecurityTracker Alert, 1010496, June 15, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	IBM[137] Directory Server 4.1, 5.1, HTTP Server 1.3.12-1.3.12 .7, 1.3.19-1.3.19 .5, 1.3.26-1.3.26 .2, 2.0.42, 2.0.42.2, 2.0.47, Tivoli Access Manager for Business Integration 5.1, Manager for e-business 3.9, 4.1, 5.1, WebSphere MQ 5.3 .0.5, 5.3 .0.1, MQ 5.3	A remote Denial of Service vulnerability exists due to an error in the IBM Global Security Toolkit (GSKit) during SSL handshakes. Updates available at: http://www-1.ibm.com/support/docview.wss?uid=swg21169222 Currently we are not aware of any exploits for this vulnerability.	IBM GSKit SSL Handshake Remote Denial of Service
Low	IRCD-Hybrid[138] ircd-ratbox ircd-hybrid 7.0.1, ircd-ratbox 1.5.1, 2.0 rc6	A remote Denial of Service vulnerability exists due to an error in the socket dequeuing mechanism. Updates available at: http://www.ircd-hybrid.org/diff/unreg_limit.diff http://www.ircd-ratbox.org/download.shtml Exploit script has been published.	Multiple ircd Socket Dequeuing Remote Denial of Service

[137] Secunia Advisory, SA11783, June 7, 2004.
[138] Bugtraq, June 18, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	Multiple Vendors[139] AVG Clam AntiVirus Computer Associates Dr. Web Frisk Software McAfee Panda RAV Symantec AVG Anti-Virus 7.0.251; Clam Anti-Virus ClamAV 0.70; Computer Associates eTrust Antivirus 6.0, InoculateIT 6.0; Dr.Web; Frisk Software F-Prot Antivirus for Linux and BSD 4.4.2; McAfee UVscan scan for Linux 4.3.20 McAfee VirusScan 6.0, VirusScan Enterprise 7.1; Panda Antivirus Platinum 2.0; RAV AntiVirus Online Virus Scan; Symantec AntiVirus for Handhelds 3.0, Norton AntiVirus 2002, 2002 Professional Edition, Norton Antivirus 2003, 2003 Professional Edition, Norton AntiVirus Corporate Edition 7.60.build 926	A remote Denial of Service vulnerability exists when certain malicious archives that contain large quantities of data are scanned. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Multiple Vendor Anti-Virus Scanner Remote Denial of Service

[139] Bugtraq, June 14, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	Multiple Vendors[140] Astaro Conectiva CRUX Debian Devil-Linux EnGarde[141] Fedora[142] Gentoo Mandrake RedHat[143] Slackware[144] SuSE[145] Trustix[146] TurboLinux[147] Wolk EnGarde Secure Community 2.0, Secure Professional 1.5; Linux kernel 2.4.18, 2.4.20-2.4.22, 2.4.25, 2.4.26, 2.6.5, 2.6.6 rc1, 2.6.6, 2.6.7 rc1	A Denial of Service vulnerability exists in the '__clear_fpu()' function in 'asm-i386/i387.h.' Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.7.tar.bz2 http://linuxreviews.org/news/2004-06-11_kernel_crash/signal.c.2.4.20.patch.tx **Engarde:** http://infocenter.guardiandigital.com/advisories/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-255.html **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Trustix:** ftp://ftp.trustix.org/pub/trustix/updates/ **TurboLinux:** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Exploit scripts have been published.	Linux Kernel Assembler Inline Function Denial of Service CVE Name: CAN-2004-0554
Low	NetBSD[148] NetBSD 1.x	A Denial of Service vulnerability exists in 'src/sys/uvm/uvm_swap.c' due to an integer overflow condition in the 'swapctl()' system call. Patches available at: http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/uvm/uvm_swap.c.diff?r1=1.85&r2=1.85.2.1 Currently we are not aware of any exploits for this vulnerability.	NetBSD Swapctl() Denial of Service
Low	OpenBSD[149] OpenBSD –current, 3.0-3.5	A remote Denial of Service vulnerability exists in the 'isakmpd' daemon due to multiple payload handling errors. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/012_isakmpd.patch Exploit scripts have been published.	OpenBSD ISAKMPD Daemon Remote Denial of Service

[140] VU#973654, http://www.kb.cert.org/vuls/id/973654.
[141] Guardian Digital Security Advisory, ESA-20040621-005, June 21, 2004.
[142] Fedora Update Notification, FEDORA-2004-171, June 14, 2004.
[143] RedHat Security Advisory, RHSA-2004:255-10, June 17, 2004.
[144] Slackware Security Advisory, SSA:2004-167-01, June 15, 2004.
[145] SUSE Security Announcement, SuSE-SA:2004:017, June 16, 2004.
[146] Trustix Security Advisory, TSLSA-2004-0034, June 16, 2004.
[147] Turbolinux Security Advisory, TLSA-2004-18, June 18, 2004.
[148] Bugtraq, June 11, 2004.
[149] SecurityFocus, June 10, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	SGI[150] IRIX 6.5.20 m, 6.5.20 f, 6.5.21 m, 6.5.21 f, 6.5.22-6.5.25	Several vulnerabilities exist: a Denial of Service vulnerability exists when a 'mapelf32exec()' call is made on a malicious binary; and a Denial of Service vulnerability exists due to page invalidation issues that exist in init. Patches available at: ftp://patches.sgi.com/support/free/security/advisories/ Currently we are not aware of any exploits for this vulnerability.	IRIX Denials Of Service CVE Names: CAN-2004-0136, CAN-2004-0137
Unavail-able	**Apple[151]** **Mac OS X 10.3-10.3.3, Mac OS X Server 10.3-10.3.3** ***US-CERT issues advisory[152]***	**Multiple vulnerabilities exist: a vulnerability exists in 'AppleFileServer' regarding the use of SSH and reporting errors; a vulnerability exists in the NFS implementation when tracing system calls; a vulnerability exists in 'LoginWindow' due to improper handling of directory service lookups and console log files; a vulnerability exists in the TCP/IP stack implementation when handling out-of-sequence TCP packets; a vulnerability exists within Terminal when handling URLs; and a vulnerability exists that involves the package installation. The impact was not specified for any of these vulnerabilities.** **Upgrades available at: http://www.apple.com/support/downloads/macosxcombined1034update.html** **http://www.apple.com/support/downloads/macosxcombinedserver1034update.html** **http://www.apple.com/support/downloads/macosxupdate_10_3_4.html** **Currently we are not aware of any exploits for this vulnerability.**	**Mac OS X Multiple Security Vulnerabilities**
High	**Gallery Project[153]** **Debian[154]** ***Gentoo[155]*** **Debian Linux 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gallery Gallery 1.4 -pl1-pl2, 1.4-1.4.3 -pl1** ***Gentoo issues advisory***	**A vulnerability exists due to an authentication error, which could let a remote malicious user obtain administrative access.** **Upgrades available at: http://prdownloads.sourceforge.net/gallery/gallery-1.4.3-pl2.tar.gz?download** **Debian:** **http://security.debian.org/pool/updates/main/g/gallery/** **There is not exploit code required.** ***Gentoo:*** **http://security.gentoo.org/glsa/glsa-200406-10.xml**	**Gallery 'init.php' Authentication Flaw**

[150] SGI Security Advisory , 20040601-01-P, June 14, 2004.
[151] Apple Security Advisory, APPLE-SA-2004-05-28, May 28, 2004.
[152] VU#174790, http://www.kb.cert.org/vuls/id/174790.
[153] Gallery Security Release, June 1, 2004.
[154] Debian Security Advisory, DSA 512-1, June 2, 2004.
[155] Gentoo Linux Security Advisory , GLSA 200406-10, June 15, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	**MIT**[156, 157] *Debian*[158] *Fedora*[159] Immunix Mandrake[160] OpenBSD *RedHat*[161] *SGI*[162] *Sun*[163] Tinysofa[164] Trustix[165] Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2.1-1.2.7, 1.3 -alpha1, 5.0 - 1.3.3, 5.0 - 1.2beta1&2, 5.0 - 1.1.1, 5.0 -1.1, 5.0 - 1.0.x; tinysofa enterprise server 1.0 -U1, 1.0 *More vendor advisories issued*	Multiple buffer overflow vulnerabilities exist due to boundary errors in the 'krb5_aname_to_localname()' library function during conversion of Kerberos principal names into local account names, which could let a remote malicious user execute arbitrary code with root privileges. Patch available at: http://web.mit.edu/kerberos/advisories/2004-001-an_to_ln_patch.txt Mandrake: http://www.mandrakesoft.com/security/advisories Tinysofa: http://www.tinysofa.org/support/errata/2004/009.html Trustix: http://http.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability. *Debian:* http://security.debian.org/pool/updates/main/k/krb5/ *Fedora:* http://securityfocus.com/advisories/6817 *RedHat:* http://rhn.redhat.com/errata/RHSA-2004-236.html *SGI:* ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ *Sun:* http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57580	Kerberos 5 'krb5_aname_to_localname' Multiple Buffer Overflows CVE Name: CAN-2004-0523
High	SquirrelMail Development Team[166] *Fedora*[167] *Gentoo*[168] Open Webmail *RedHat*[169] *SGI*[170] SquirrelMail 1.4-1.4.3 RC1, 1.5 Development Version; Open Webmail 2.30-2.32 *Vendors issue advisories*	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied e-mail header strings, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.squirrelmail.org/download.php There is not exploit code required; however, a Proof of Concept exploit has been published. *Fedora:* http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ *Gentoo:* http://security.gentoo.org/glsa/glsa-200406-08.xml *RedHat:* http://rhn.redhat.com/errata/RHSA-2004-240.html *SGI:* ftp://patches.sgi.com/support/free/security/patches/ProPack/3/	SquirrelMail Cross-Site Scripting CVE Name: CAN-2004-0520

[156] MIT krb5 Security Advisory 2004-001, June 3, 2004.
[157] TA04-147A, http://www.kb.cert.org/vuls/id/686862.
[158] Debian Security Advisory DSA 520-1, June 16, 2004.
[159] Fedora Update Notification, FEDORA-2004-149 & 150, June 4, 2004.
[160] Mandrakelinux Security Update Advisory, MDKSA-2004:056, June 3, 2004.
[161] RedHat Security Advisory, RHSA-2004:236-14, June 9, 2004.
[162] SGI Security Advisories, 20040604-01-U & 20040605-01-U, June 21, 2004.
[163] Sun(sm) Alert Notification, 57580, June 10, 2004.
[164] Tinasofa Security Advisory, TSSA-2004-009, June 2, 2004.
[165] Trustix Security Advisory, TSLSA-2004-0032, June 2, 2004.
[166] RS-2004-1, May 30, 2004.
[167] Fedora Update Notification, FEDORA-2004-160, June 9, 2004.
[168] Gentoo Linux Security Advisory, GLSA 200406-08, June 15, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	Tripwire, Inc.[171] Gentoo[172] *Mandrake*[173] Tripwire 2.2.1, 2.3.0, 2.3.1 -2, 2.3.1, 2.4 .0, 2.4.2, 3.0 1, 3.0, 4.0, 4.0.1, 4.1, 4.2, Tripwire Open Source 2.3.0, 2.3.1 *Mandrake issues advisory*	A format string vulnerability exists in 'pipedmailmessage.cpp' when an e-mail report is generated, which could let a malicious user execute arbitrary code. *Note: It is reported that this issue only presents itself when the MAILMETHOD is sendmail.* Patch available at: http://securityfocus.com/bid/10454/solution/ Gentoo: http://security.gentoo.org/glsa/glsa-200406.02.xml Currently we are not aware of any exploits for this vulnerability. *Mandrake:* http://www.mandrakesoft.com/security/advisories	Tripwire Email Reporting Format String
High/Low (High if arbitrary code can be executed)	Firebird[174] *Borland/Inprise* Firebird 1.0 *Borland/Inprise Interbase 4.0, 5.0, 6.0, 6.4, 6.5, 7.0, 7.1, InterBase SuperServer 6.0* *Exploit script published*[175]	A buffer overflow vulnerability exists when handling database names due to insufficient boundary checks, which could let a remote malicious user cause a Denial of Service and ultimately execute arbitrary code. Upgrade available at: http://firebird.sourceforge.net/index.php?op=files&id=engine A Proof of Concept exploit has been published.	Firebird Remote Database Name Buffer Overflow
Medium	BEA Systems Inc.[176] WebLogic Server and WebLogic Express *US-CERT issues advisory*[177]	A vulnerability that occurs when a weblogic.xml file is edited through Weblogic Builder or the SecurityRoleAssignmentMBean may allow unintended access to web applications. Patch available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_59.00.jsp	Weblogic & Web Express Unauthorized Access CVE Name: CAN-2004-0470

[169] RedHat Security Advisory, RHSA-2004:240-06, June 14, 2004.
[170] SGI Security Advisory , 20040604-01-U, June 21, 2004.
[171] SecurityFocus, June 5, 2004.
[172] Gentoo Linux Security Advisory, GLSA 200406-02, June 4, 2004.
[173] Mandrakelinux Security Update Advisory , MDKSA-2004:057, June 8, 2004.
[174] Securiteam, June 1, 2004.
[175] SecurityFocus, June 12, 2004.
[176] BEA Security Advisory: (BEA04-59.00), May 11, 2004
[177] VU#950070, http://www.kb.cert.org/vuls/id/950070.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	**GNU**[178] **Conectiva** [179] ***Gentoo***[180] **Mandrake**[181] **Mailman 1.0, 1.1, 2.0 beta 3-beta 5, 2.0-2.0.13, 2.1, 2.1b1, 2.1.1-2.1.4** ***Gentoo issues advisory***	**A vulnerability exists because a remote malicious user can send a specially crafted e-mail request to the mailman server to retrieve the mailman password of a target mailman subscriber.** **Upgrade available at:** **http://prdownloads.sourceforge.net/mailman/mailman-2.1.5.tgz?download** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/9/RPMS/mailman-2.1.4-27744U90_2cl.i386.rpm** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Currently we are not aware of any exploits for this vulnerability.** ***Gentoo:*** **http://security.gentoo.org/glsa/glsa-200406-04.xml**	**GNU Mailman Password Retrieval** **CVE Name: CAN-2004-0412**

Multiple/Other Operating Systems

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	EDIMAX Technology Co.[182] Edimax 7205APL 2.40 a-00	A vulnerability exists due to a default backdoor account that is hard coded and cannot be removed, which could let a remote malicious user obtain sensitive information and log into the device as administrator. No workaround or patch available at time of publishing. There is no exploit code required.	Edimax EW-7205APL Default Account & Password Disclosure
High	Infoblox, Inc. [183] DNS One Appliance 2.4 .0-8A, 2.4 .0-8	A vulnerability exists due to insufficient filtering of the 'HOSTNAME' and 'CLIENTID' DHCP options before displaying information based on those fields in an administrative report, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	DNS One Appliance Input Validation
High	Linksys[184] Web Camera Software 2.10	A Cross-Site Scripting vulnerability exits in the 'next_file' parameter in the 'main.cgi' script, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Linksys Web Camera Software Cross-Site Scripting

[178] SecurityTracker Alert, 1010283, May 25, 2004.
[179] Conectiva Linux Security Announcement, CLA-2004:842, May 25, 2004.
[180] Gentoo Linux Security Advisory, GLSA 200406-04, June 9, 2004.
[181] Mandrakelinux Security Update Advisory, MDKSA-2004:051, May 26, 2004.
[182] Bugtraq, June 10, 2004.
[183] SecurityFocus, June 19, 2004.
[184] Bugtraq, June 13, 2004.

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
High	Novell[185] iChain Server 2.2 SP1, 2.2 FP1a, 2.2 FP1, 2.2, 2.3	A Cross-Site Scripting vulnerability exists due to insufficient filtering of the 'url' parameter to remove HTML code from user-supplied HTTP POST requests, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10090234.htm There is no exploit code required.	Novell iChain Cross-Site Scripting
High	U.S.Robotics[186] Broadband Router 8003	An information disclosure vulnerability exists in the administrative web interface during authentication because the administrator password can be read in plaintext, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	U.S. Robotics Broadband Router 8003 Administration Web Interface
High/ Medium (Medium if memory can be corrupted)	Skype Technologies S.A.[187] Skype 0.98.0.04	A buffer overflow vulnerability exists in 'callto://' URI data due to insufficient bounds checking, which could let a remote malicious user corrupt sensitive regions of memory and possibly execute arbitrary code. Upgrade available at: http://www.skype.com/download.html Currently we are not aware of any exploits for this vulnerability.	Skype CallTo URI Handler Buffer Overflow
High/ Low (Low if a DoS)	VICE[188] VICE 1.6, 1.13, 1.14	A format string vulnerability exists in the handling of the monitor 'memory dump' command, which could let a malicious user cause a Denial or Service or execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	VICE Monitor Memory Dump Format String CVE Name: CAN-2004-0453
Medium	Billion Electric Co. Ltd.[189] BIPAC-640 AE 3.33	A vulnerability exists due to an error when processing HTTP requests, which could let a remote malicious user bypass the user authentication on the administrative web interface. Upgrade available at: http://www.billion.com/support/download/fd/BIPAC-640_AE/BIPAC-640AEv335.zip There is no exploit code required.	Billion BIPAC 640 AE Authentication Bypass
Medium	Blackboard, Inc.[190] Blackboard 6.0	A vulnerability exists in 'Digital Dropbox' due to insufficient authorization, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Blackboard Learning System 'Digital Dropbox' Information Disclosure

[185] Novell Technical Information Document, TID10080762, June 17, 2004.
[186] Secunia Advisory, SA11812, June 10, 2004.
[187] SecurityFocus, June 10, 2004.
[188] VICE Security Advisory, VSA-2004-1, June 13, 2004.
[189] Secunia Advisory, SA11813, June 10, 2004.
[190] Bugtraq, June 10, 2004.

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	Linksys[191] Web Camera Software 2.10	A Directory Traversal vulnerability exists because it is possible to disclose the content of arbitrary files by passing their path to the 'next_file' parameter in 'main.cgi,' which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Linksys Web Camera Software Directory Traversal
Medium	Microsoft[192] Apple Opera Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, SP1 & SP2, 6.0, SP1; Internet Explorer Macintosh Edition 5.0 MRJ 2.2, MRJ 2.1.4, 5.0, 5.1, 5.1.1, 5.2.2; Opera Software Opera Web Browser 7.51	A vulnerability exists due to an error when handling URLs, which could let a remote malicious user bypass security zones or conduct phishing attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer URI Obfuscation
Medium	Symantec[193] Gateway Security 360R 2.1 Build 415, 360R 2.1 Build 300	A vulnerability exists because not-VPN packets can be sent via the wireless interface to the internal LAN even if the 'Enforce VPN Tunnels/Disallow IPSec pass thru' and 'Enforce VPN Tunnels/Allow IPSec pass thru' settings are configured, which could let a remote malicious user bypass security access controls. No workaround or patch available at time of publishing. There is no exploit code required.	Symantec Gateway Security 360R Wireless VPN Bypass
Low	Cisco Systems[194, 195] Catalyst 6000 series, 5000 series, 4500 series, 4000 series, 2948G, 2980G, 2980G-A, 4912G, 2901, 2902, 2926[T,F,GS,GL], 2948	A remote Denial of Service vulnerability exists when a malicious user submits an invalid packet instead of the final ACK packet during a 3-way handshake. Workarounds and updates available at: http://www.cisco.com/warp/public/707/cisco-sa-20040609-catos.shtml There is no exploit code required.	CatOS TCP-ACK Remote Denial Of Service CVE Name: CAN-2004-0551

[191] Bugtraq, June 7, 2004.
[192] Bugtraq, June 10, 2004.
[193] Bugtraq, June 9, 2004.
[194] Cisco Security Advisory , 52781, June 9, 2004.
[195] VU#245190, http://www.kb.cert.org/vuls/id/245190.

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	Cisco Systems[196, 197] IOS 11.x, 12.x, R11.x, R12.x	A remote Denial of Service vulnerability exists when the device is configured to support Border Gateway Protocol (BGP) packets and a remote malicious user submits a specially crafted BGP packet. Patches available at: http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS Border Gateway Protocol Remote Denial of Service
High	**SMC Networks[198]** **SMC Broad-band Router SMC7008ABR (1.032, SMC7004VBR (1.231)** ***Update now available[199]***	**A vulnerability exists because the default configuration does not set a password, which could let a remote malicious user unauthorized administrative access.** **No workaround or patch available at time of publishing.** **There is no exploit code required.** ***Update available at:*** **http://www.smc.com/index.cfm?sec=Support&pg=Download-Details?=243&site=c**	**SMC Broadband Routers Unauthorized Administrative Access**

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[196] Cisco Security Advisory , 53021, June 16, 2004.
[197] VU#784540, http://www.kb.cert.org/vuls/id/784540.
[198] Bugtraq, April 28, 2004.
[199] SecurityFocus, June 7, 2004.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 8 and June 22, 2004, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period 30 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 22, 2004	Code.zip	Some bits of code that show how modified URL encoding can easily bypass restricted zones via Microsoft Internet Explorer.
June 19, 2004	H7kill.c	Script that exploits the Multiple IRCD Socket Dequeuing Denial of Service vulnerability.
June 18, 2004	Cifspwscan-1_0_3.tar.gz	A CIFS/SMB password scanner based on the jcifs implementation.
June 18, 2004	dnsPoison.cpp.txt	Proof of Concept exploit for the Symantec Enterprise Firewall DNSD DNS Cache Poisoning vulnerability.
June 18, 2004	Ettercap-NG-0.7.0_rc1.tar.ga	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
June 18, 2004	Flawfinder-1.26.tar.gz	Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first.
June 18, 2004	Sqlat-src-1.1.0.tar.gz	A suite of tools that does dictionary attacks, upload files, read registry and dump the SAM.
June 17, 2004	Whopper.pl	A simple yet powerful tool used to connect to remote services through a chain of HTTP (CONNECT) proxy servers for the sole purpose of gaining a higher level of anonymity.
June 15, 2004.	Symantec_enterprise_fw_dnsd_ poison.cpp	Proof of Concept exploit script for the Symantec Enterprise Firewall DNSD DNS Cache Poisoning vulnerability.
June 15, 2004	**X_hpux_xfs.pl**	**Perl script that exploits the HP-UX Local X Font Server Buffer Overflow vulnerability.**
June 14, 2004	**blackboardLS.txt**	**Exploit for the Blackboard Learning System 'Digital Dropbox' Information Disclosure vulnerability.**
June 14, 2004	**Freeips-dos.c**	**Proof of Concept exploit for the FreeIPS Protected Service Remote Denial of Service vulnerability.**
June 14, 2004	Hping3-alpha-1.tar.gz	A network tool designed to send custom ICMP/UDP/TCP packets and to display target replies like ping. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under all supported protocols. Using hping, you can test firewall rules and perform spoofed port scanning.

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 14, 2004	kernelInlineASMDoS.c	Script that exploits the Linux Kernel Assembler Inline Function Local Denial Of Service vulnerability.
June 14, 2004	kernelInlineASMDoSDetail.c	Script that exploits the Linux Kernel Assembler Inline Function Local Denial Of Service vulnerability.
June 14, 2004	sygateFW.txt	Proof of Concept script that exploits the Sygate Personal Firewall Pro Local Fail-Close Bypass vulnerability.
June 14, 2004	Weplab-0.0.2b-alpha.tar.gz	A tool to review the security of WEP encryption in wireless networks that includes several attacks to help measure the effectiveness and minimum requirements necessary to succeed.
June 14, 2004	**WinAgentsTFTP.txt**	**Exploit for the WinAgents TFTP Server Remote Buffer Overflow vulnerability.**
June 11, 2004	**WinagentDos.pl**	**Perl script that exploits the Remote Denial of Service**
June 12. 2004	priv8ibserverb.pl	Perl script that exploits the Firebird Remote Database Name Buffer Overflow vulnerability.
June 10, 2004	**Blackboard_exploit.pl**	**Proof of Concept exploit for the Blackboard Learning System 'Digital Dropbox' Information Disclosure vulnerability.**
June 10, 2004	Framework-2.1.tar.gz	An advanced open-source platform for developing, testing, and using exploit code. This release includes 18 exploits and 27 payloads.
June 10, 2004	Isakmpd-piggyback-delete-payload.sh	Exploit for the OpenBSD ISAKMPD Daemon Remote Denial of Service vulnerability.
June 10, 2004	Isakmpd-piggyback-delete-payload-v2.sh	Exploit for the OpenBSD ISAKMPD Daemon Remote Denial of Service vulnerability.
June 10, 2004	Modproxy1.html	Proof of Concept exploit script for the Apache Mod_Proxy Remote Negative Content-Length Buffer Overflow Vulnerability.
June 10, 2004	Squid_ntlm_authenticate.pm	Exploit for the quid Proxy NTLM Authentication Buffer Overflow vulnerability.
June 9, 2004	Imperva.crystal2.tx	Exploit for the Crystal Reports Web Viewer Directory Traversal vulnerability.
June 9, 2004	Priv8ibserver.pl	Perl script that exploits the Firebird Remote Database Name Buffer Overflow vulnerability.
June 9, 2004	**Rdboom.zip**	**Remote Denial of Service proof of concept exploit that makes use of a flaw in the Race Driver.**
June 8, 2004	**tocaRaceDriverDOSexp.zip**	**Exploit for the TocToCA Race Driver Multiple Remote Denial of Service vulnerabilities.**

Trends

- Cabir is the first-ever computer virus that is capable of spreading over mobile phone networks. It is a network worm that infects phones running the Symbian mobile phone operating system by Symbian.
- **US-CERT has received reports of scanning activity directed at port 5000/tcp. This port is used by the Microsoft Windows Universal Plug and Play service (UPnP). There are known vulnerabilities in UPnP, for which a patch has been available (Microsoft Security Bulletin MS01-059).**
- **US-CERT has received reports of a new worm, referred to as "W32/Sasser." This worm attempts to take advantage of a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). See Microsoft Security Bulletin located at: http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx. The vulnerability allows a remote malicious user to execute arbitrary code with SYSTEM privileges. There are several variants of this worm circulating in the wild. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **Fraudulent e-mails designed to dupe Internet users out of their credit card details or bank information topped the three billion mark last month, according to one of the largest spam e-mail filtering companies. The authentic-looking e-mails, masquerading as messages from banks or online retailers, have become a popular new tool for tech-savvy fraudsters in a new scam known as "phishing."**

Viruses/Trojans

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Netsky-B	Win32 Worm	Slight Increase	February 2004
2	W32/Netsky-D	Win32 Worm	Slight Decrease	March 2004
3	W32/Netsky-P	Win32 Worm	New to Table	March 2004
4	W32/Netsky-Q	Win32 Worm	New to Table	March 2004
5	W32/Netsky-Y	Win32 Worm	New to Table	April 2004
6	W32/Netsky-C	Win32 Worm	Decrease	March 2004
7	W32/Bagle	Win32 Worm	Decrease	April 2004
8	W32/Netsky-Z	Win32 Worm	New to Table	April 2004
9	W32/Sasser	Win32 Worm	New to Table	April 2004
10	W32/Netsky.AA	Win32 Worm	New to Table	April 2004

The following table encompass new viruses, variations of previously encountered viruses, and Trojans that have been discovered in the last two weeks. They are listed alphabetically by their name. While these viruses and Trojans might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. Readers should also contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Following this table are write-ups of new viruses and Trojans that are considered to be a high level threat. *NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

Name	Aliases	Type
Backdoor.Berbew.E		Trojan
Backdoor.Hacarmy.C		Trojan
Backdoor.Nibu.H	TrojanSpy.Win32.Dumarin.c	Trojan
Backdoor.Ranky.G	Proxy-FBSR	Trojan
Backdoor-CGB		Trojan
Download.Ject		Trojan
Downloader-IQ		Trojan
Downloader-KY		Trojan
Downloader-LC		Trojan
Downloader-LE		Trojan
Hombia	BAT.Hombia	Batch File Virus
JS/Exploit-DialogArg.a		Trojan
JS/Keylog-Briss.ldr		Trojan
JS/Stealus	JS/Stealus.gen	Trojan
PWS-Respa		Trojan
PWSteal.Bamer.A	PWS:Win32/Bamer	Trojan
StartPage-DC!hosts		Trojan
StartPage-DP		Trojan
StartPage-DQ		Trojan
StartPage-DQ		Trojan
StartPage-DU		Trojan
Symb/Cabir-A	Cabir Epoc.Cabir EPOC/Cabir.A Worm.Symbian.Cabir.a Symbian/Cabir.b EPOC_CABIR.A Symbian/Cabir EPOC_CABIR Worm.Symbian.Cabir	Symbian Bluetooth Worm
Troj/Sober-H	WORM_SOBER.H Trojan.Ascetic.A W32.Sober.H@mm W32/Sober.h	Trojan
Trojan.Boxed.A	DDos.Win32.Boxed.d	Trojan
Trojan.Boxed.B	DDos.Win32.Boxed.c	Trojan
Trojan.Gletta.A		Trojan

Name	Aliases	Type
Trojan.Wintrash		Trojan
VBS/Pub-A	VBS_PUB.A	Visual Basic Script Worm
W32.Gaobot.AQS		Win32 Worm
W32.Paps.A@mm		Win32 Worm
W32.Tubty.A@mm		Win32 Worm
W32/Agobot-JP	Backdoor.Agobot.gen W32/Gaobot.worm.gen.d virus W32.HLLW.Gaobot.gen WORM_AGOBOT.IY	Win32 Worm
W32/Agobot-JT		Win32 Worm
W32/Agobot-JW		Win32 Worm
W32/Agobot-JX		Win32 Worm
W32/Agobot-KB	Backdoor.Agobot.gen W32/Gaobot.worm.gen.g virus W32.HLLW.Gaobot.gen	Win32 Worm
W32/Agobot-WR		Win32 Worm
W32/Dansh-A	Kobot W32/Dansh.worm!irc W32.Kobot.A Win32.HLLW.Shodan WORM_DANSH.A	Win32 Worm
W32/Korgo.worm.r		Win32 Worm
W32/Korgo-P	W32/Korgo.worm.p W32//Korgo.L W32/Korgo.N.worm Worm.Win32.Padobot.g	Win32 Worm
W32/Lovgate-V	I-Worm.LovGate.w W32.Lovgate.Gen@mm WORM_LOVGATE.V	Win32 Worm
W32/Plexus.b@MM	MultiDropper-KR	Win32 Worm
W32/Rbot-AA	Backdoor.Rbot.gen, W32/Sdbot.worm.gen.g virus, W32.Spybot.Worm	Win32 Worm
W32/Rbot-AE	Backdoor.Rbot.gen W32/Sdbot.worm.gen.o virus W32.Spybot.Worm	Win32 Worm
W32/Rbot-AQ	Backdoor.Rbot.gen W32/Sdbot.worm.gen.o W32.Spybot.Worm WORM_SDBOT.OA	Win32 Worm
W32/Rbot-AS		Win32 Worm
W32/Rbot-AV	Backdoor.Rbot.e, W32/Gaobot.worm.gen.e virus W32.Spybot.Worm	Win32 Worm
W32/Rbot-AX	Backdoor.Rbot.gen W32.Spybot.Worm WORM_AGOBOT.XP	Win32 Worm
W32/Rbot-AY	Backdoor.Rbot.gen W32/Gaobot.worm.gen.f W32.Spybot.Worm	Win32 Worm
W32/Rbot-BC		Win32 Worm
W32/Rbot-BI		Win32 Worm
W32/Rbot-BL	W32/Sdbot.worm.gen.g	Win32 Worm
W32/Sdbot-JB	W32.Randex.gen WORM_SDBOT.CT	Win32 Worm
W32/Setclo.worm		Win32 Worm

Name	Aliases	Type
W32/Spybot-CO	Worm.P2P.SpyBot.gen W32/Spybot.worm.gen.f Win32/SpyBot.TE W32.Spybot.Worm	Win32 Worm
W32/Zafi-B	I-Worm.Zafi.b W32/Zafi.b@MM Win32/Zafi.B W32.Erkez.B@mm PE_ZAFI.B Win32.Hazafi.30720	File Infector
W97M.Anisc	Macro.Word97.Anesc	Word 97 Macro Virus
W97M.MLHR		Word 97 Macro Virus
WORM_KORGO.L	W32/Korgo.L UnivAP.E Worm.Win32.Korgo.9728 W32.Korgo.L W32.Korgo.I W32/Korgo.N.worm Worm.Win32.Padobot.g W32/Korgo.worm.p	Win32 Worm
WORM_KORGO.M	W32/Korgo.M Univ.AP.E Win32:Korgo-K [Wrm] Worm.Win32.Korgo.9728	Win32 Worm
WORM_KORGO.Q	W32/Korgo.worm.q	Win32 Worm
WORM_LOVGATE.AB	32/Lovgate.ab@MM Win32:Lovgate-AB [Wrm] Win32/Lovgate.AC@mm I-Worm.LovGate.ac Worm/LovGate.AS I-Worm/Lovgate.Z I-Worm.Win32.Lovgate.108544	Win32 Worm
WORM_RBOT.AF		Internet Worm
WORM_SDBOT.FO		Internet Worm
WORM_SDBOT.RZ		Internet Worm
X97M.Crex		Excel 97 Macro Virus